PRIVACY IMPACT ASSESSMENT
Crisis Response System

1. **Department of Defense Component:** Defense Logistics Agency.

2. **Name of IT System:** Crisis Response System.

3. **Budget System Identification Number:** N/A.

4. **System Identification Number(s) (IT Registry/Defense IT Portfolio Repository):** N/A.

5. **IT Investment Unique Identifier (OMB Circular A-11):** N/A.

6. **Privacy Act System of Records Notice Identifier:** DLA Privacy Act System of Records S900.10, entitled "Personnel Roster/Locator Files".

7. **OMB Information Collection Requirement Number and Expiration Date:** N/A.

8. **Authority to collect information:** Defense Supply Center Columbus Continuity of Operations Plan and references therein; Occupant Emergency Plan, Defense Logistics Agency, Defense Supply Center Columbus.

9. **Brief summary or overview of the IT system:** The system is a database application that is used to provide information regarding the status of persons working on base at the Defense Supply Center Columbus, when and if a crisis occurs on the Center. The status includes whether a person is injured, dead, available for work, or the status is unknown; and whether the status is confirmed or unconfirmed. The information gathered would be provided to and also received from management. Information would also be gathered from other sources and provided to emergency contacts. The program utilizes data feeds from the Defense Civilian Personnel Data System, the Electronic Official Personnel File, the Corporate Database, and the Lenel System. When used during a crisis, it will provide accountability information to DLA management regarding availability of personnel and a record of contacts. The Crisis Response Team is the controlling unit for the system.

10. **Identifiable Information to be Collected and Nature / Source:** Information collected for DLA employees includes: name, organization, occupational series, and location on Center, user ID, work phone, status, and contacts. Information collected for non-DLA employees includes: name, location, work phone, title, and status. The information collected comes from the data feeds listed above. During a crisis, information will also come from people reporting the status of individuals and from people reporting contacts made.

11. **Method of information collection:** Information collected is via paper, in person, telephonic, and electronic.

12. **Purpose of the collection:** The information collected is to provide continuity of work during an emergency on Center. It is a tool that provides reporting capability of who is or is not available for work by name and/or by occupation and/or by organization and/or by location, as well as who is not accounted for. It also provides a repository of emergency contacts made and received.

13. **Data uses:** Data is used as a management tool to determine personnel available for work during a crisis. It is also used for notification to emergency contacts.

14. **Does system derive / create new data about individuals through aggregation?** Other than collecting the status of an individual during a crisis and recording contacts made, no new or previously unavailable information is created.

15. **Internal and External Sharing:**
Internal to DLA: Internally, data will be shared with management.
External to DLA: Externally, status of individuals during a crisis will be shared with listed emergency contacts. Data may also be provided under any of the routine uses published in the system of records notice and/or the DOD "Blanket Routine Uses" published at http://www.defenselink.mil/privacy/notices/blanket-uses.html .

16. **Opportunities to object to the collection or to consent to the specific uses and how consent is granted:** The information that is provided through the database feeds has been originally collected with Privacy Act statements. Emergency contact information is provided voluntarily.

17. **Information provided the individual at Collection, the Format, and the Means of delivery:** Privacy Act system of records notices were published for the original collection databases. Further, the DLA Code of Fair Information Principles governs all Privacy Act data collection. The principals are contained in DLA Privacy Act training modules which are mandatory trainings for all DLA civilian employees, military members, and contractors. The DLA workforce is required to be aware of the principals to fulfill their duties in handling third party personal data and in learning their Privacy Act rights.

18. **Data Controls:**
Administrative: Users are those who must use the records to perform their duties in a crisis and are designated to have access to the application. These users are required to receive Privacy Act and Information Assurance initial and refresher trainings.
Physical: The program and data is on discs that are stored in secured safes on Center. It is also on a system that is not connected to the World Wide Web.
Technical: Access is restricted by the use of logons and passwords. Electronic records are on an accredited system. DLA computer safeguard protocols are applicable.

19. **Privacy Act Interface:** The fields in the accountability program are listed in the categories of records for the DLA Master Database and the decentralized systems. The program is covered under the Privacy Act system of records, S900.10

20. **Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures:**

Data sharing internally occurs among individuals authorized to have access to the system information. System users are made aware of restrictions on secondary uses of the data by initial and refresher Privacy Act and Information Assurance trainings.

Presently, no dangers are known in providing individuals an opportunity to object or consent or in notifying individuals.

The security risks are minimized by the safeguards described in this document. The safes are maintained by Security or by Command Control personnel. Data access is limited by logons, passwords, and unavailability to the World Wide Web. Data is available to only those whose job performances require access.

21. **Classification and Publication of Privacy Impact Assessment:**
Classification: Unclassified.
Publication: This document will be posted either in full or in summary form on the DLA public website, http://www.dla.mil/public_info/efoia/privacy.asp .

DATA OWNER:
Name: [redacted] (Signature) February 7, 2008 (Date)
Title: Associate General Counsel [redacted]
Work Telephone Number: [redacted]

INFORMATION ASSURANCE MANAGER: [redacted] (Signature) February 7, 2008 (Date)
Name: [redacted]
Title: Information Assurance Manager
Work Telephone Number: [redacted]
Email: [redacted]

CHIEF PRIVACY OFFICER: [redacted] (Signature) 25 Feb 2008 (Date)
Name: Lewis Oleinick
Title: Chief Privacy and FOIA Officer
Work Telephone Number: [redacted]
Email: [redacted]

REVIEWING OFFICIAL: [redacted] (Signature) MAR 18 2008 (Date)
Name: Mae De Vincentis
Title: DLA Chief Information Officer
Work Telephone Number: [redacted]
Email: [redacted]